UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,911	07/05/2003	Alexander Medvinsky	018926-010400US	4648

37490 7590 05/26/2005

CARPENTER & KULAS, LLP
1900 EMBARCADERO ROAD
SUITE 109
PALO ALTO, CA 94303

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/613,911	MEDVINSKY, ALEXANDER	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 are pending in this office action.

2. Applicant's arguments, filed April 6, 2005, with respect to claims 1-13 have been considered but are moot in view of the new ground(s) of rejection.

Specification

3. The specification is objected to because on page 1, "Serial No. _____" should be "Serial No. 10/613,868."

Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

5. Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parks et al. (U.S. Patent Pub. No. 2003/0233553) in view of Sirbu et al. (U.S. Patent No. 5,809,144).

Regarding claim 1, Parks et al. teaches a method for providing a secure time signal from a time source to a time requestor over a digital network, the method comprising:

- Using an information object to request the secure time signal (page 4, paragraph 0039 and 0040) wherein the information object includes an identification of the requestor and a session key for transferring the secure time signal (page 4, paragraph 0039, this paragraph shows how an identification of the requestor is found based on the signed messages and/or certificates).

Parks et al. does not teach **sending a requestor identification to an authentication server and** wherein the information object includes a session key for transferring the secure time signal.

Sirbu et al. teaches **sending a requestor identification to an authentication server and** wherein the information object includes a session key for transferring the secure time signal (col. 12, lines 45-54). See the attached document about Kerberos. Namely, the end of the first page and beginning of the second page, where it states Kerberos utilizes a session key created by the Ticket Granting Server and sent back to the workstation as a ticket. Also, page 1, second and third paragraph of Kerberos document, says that the workstation supplies requestor identification to an authentication server in the form of user-id and password.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein the information object includes a session key for transferring the secure time signal, as taught by Sirbu et al. with the

apparatus/medium of Parks et al. It would have been obvious for such modifications because session keys are more suited in a case where a time object is only required sporadically (once every minute, hour, day, etc.); whereby a single set of keys is used to obtain the time object, and once obtained, the keys can be destroyed. This prevents an attacker from learning the key through multiple uses, which would then allow the attacker to change the time and a digital rights content.

Regarding claim 2, the combination of Parks et al. in view of Sirbu et al. teaches wherein the information object includes a ticket (see col. 12, lines 45-54 of Sirbu et al.).

Regarding claims 3-5, the combination of Parks et al. in view of Sirbu et al. teaches wherein the ticket is obtained from a key distribution center, from an authentication server, or from a ticket-granting-server (see col. 12, lines 45-54 of Sirbu et al.).

Regarding claim 6, the combination of Parks et al. in view of Sirbu et al. teaches further comprising:

- Associating a request for a secure time signal with the ticket (see col. 10, lines 12-16 of Sirbu et al.);
- Transferring the ticket with the request to a secure time server (see col. 10, lines 4-16 of Sirbu et al.); and

- Receiving a secure time signal from the secure time server (see page 4, paragraph 0042 through page 4, paragraph 0048 of Parks et al.).

Regarding claim 7, the combination of Parks et al. in view of Sirbu et al. teaches wherein the request includes a request message, the method further comprising:

- Generating a nonce to be included in the request message (see col. 10, lines 4-7 of Sirbu et al.);
- Including a service ticket for the secure time server in the request message (see col. 10, lines 12-16 of Sirbu et al.); and
- Including a keyed checksum over the request message (see col. 10, lines 4-7 of Sirbu et al.).

Regarding claim 8, the combination of Parks et al. in view of Sirbu et al. teaches wherein the secure time signal includes a reply message, the method further comprising:

- Including a secure time signal (see page 4, paragraph 0042-0048 of Parks et al.);
- Including a nonce copied from the client request (see col. 14, lines 58-67 of Sirbu et al.); and
- Including a keyed checksum over the reply message (see col. 14, lines 58-67 of Sirbu et al.).

Regarding claim 9, the combination of Parks et al. in view of Sirbu et al. teaches wherein the step of receiving a secure time signal includes the following substeps:

- Matching a nonce in the received message with the corresponding nonce in the sent message (see col. 15, lines 1-9 of Sirbu et al.); and
- Confirming a keyed checksum (see col. 15, lines 1-9 of Sirbu et al.).

Regarding claim 10, the combination of Parks et al. in view of Sirbu et al. teaches further comprising using the secure time signal to update a clock value (see page 3, paragraph 0034 of Parks et al.).

Regarding claims 11-13, Parks et al. teaches an apparatus/computer-readable medium for providing a secure time signal to a time requestor over a digital network, the apparatus comprising:

- A process for accepting a ticket from the time requestor to request a secure time signal (page 4, paragraph 0039 and 0040); and
- A process for providing a secure time signal to the time requestor (page 4, paragraph 0042-0048).

Parks et al. does not teach **a process for sending a requestor identification to an authentication server**.

Sirbu et al. teaches **a process for sending a requestor identification to an authentication server** (col. 12, lines 45-54). See the attached document about Kerberos. Namely, page 1, second and third paragraph of Kerberos document, says that the workstation supplies requestor identification to an authentication server in the form of user-id and password.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine sending a requestor identification to an authentication server, as taught by Sirbu et al. with the apparatus/medium of Parks et al. It would have been obvious for such modifications because the identification ensures the request has come from someone that says they are (see page 1, second paragraph of attached Kerberos document).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100